National Cybersecurity Center of Excellence (NCCoE)
Energy Sector

Energy Provider Community of Interest

22 September 2016

NIST National Institute of Standards and Technology U.S. Department of Commerce

NCCoE NATIONAL CYBERSECURITY CENTER OF EXCELLENCE

Agenda

- NCCoE Energy Sector News
- Current Projects
  - Identity and Access Management (IdAM) Project Update
  - Situational Awareness (SA) Project Update
- Oil and Natural Gas Project Concepts
- Oil and Natural Gas Use Case Development Discussion

NCCoE Out and About:

- Upcoming planned conferences
  - GridSecCon
    - October 17, 2016 in Quebec City
    - *4 hour workshop:* http://www.nerc.com/pa/CI/CIPOutreach/Pages/GridSecCon-Training-Tracks.aspx
    - *Topics include:*
      - NIST NCCoE overview, including Cyber Security Framework
      - Top challenges in the industry from industry, association, and integrator perspective
      - NCCoE Solutions
  - 11th Annual Cybersecurity Conference for the Oil & Natural Gas Industry
    - November 9, 2016 in Houston

CURRENT PROJECTS: IDAM

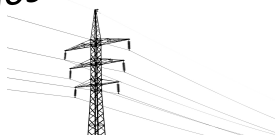
Challenges we heard from industry:

- **Lack of authentication, authorization, and access control requirements for all OT**
- **Inability to manage and log authentication, authorization, and access control information for all OT using centralized or federated controls**
- **Inability to centrally monitor authorized and unauthorized use of all OT and user accounts**
- **Inability to provision, modify, or revoke access throughout the enterprise (including OT) in a timely manner**

Solution NCCoE built:

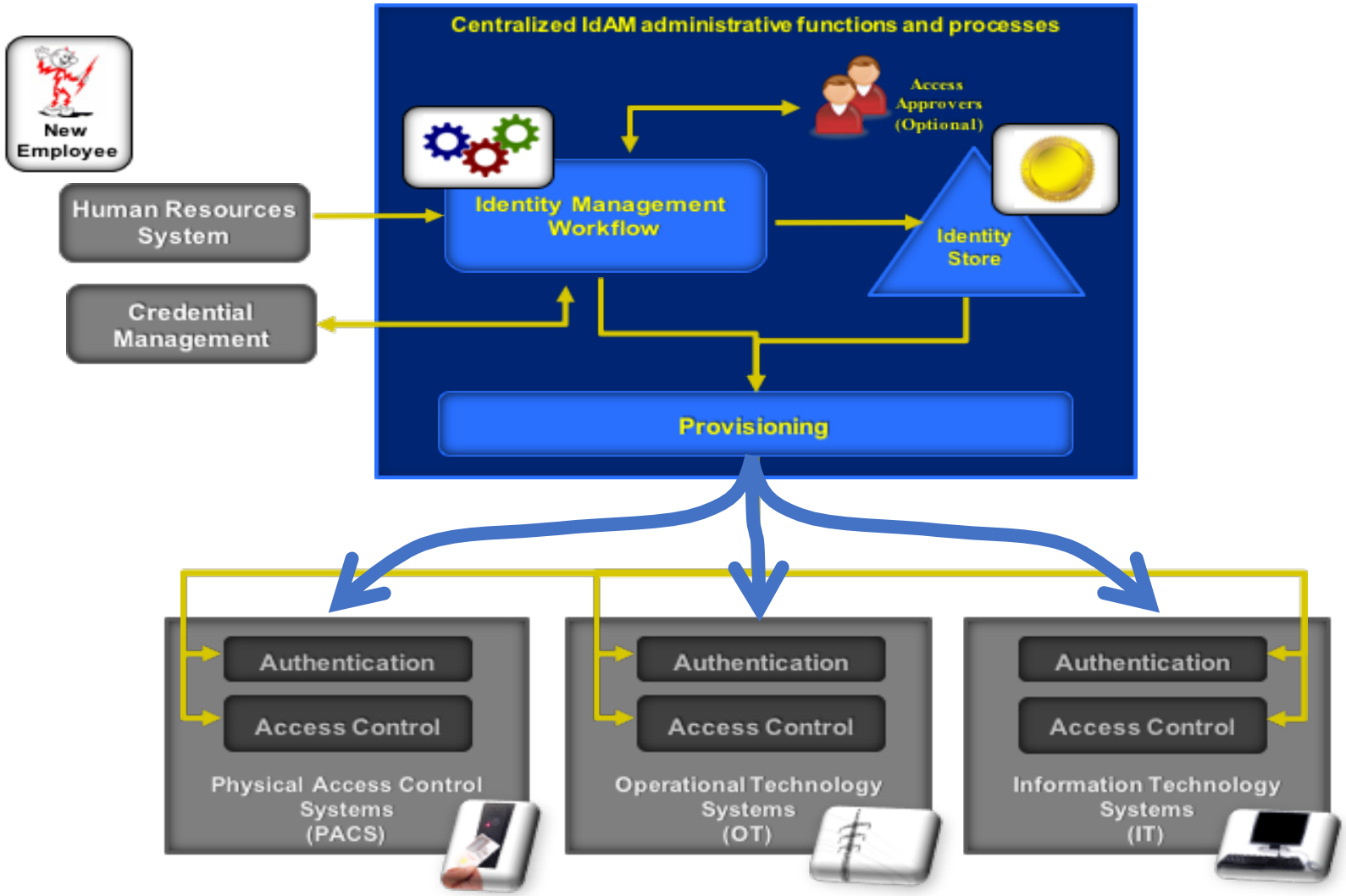
- ✓ Authenticates individuals and systems
- ✓ Enforces authorization control policies
- ✓ Unifies IdAM services
- ✓ Protects generation, transmission and distribution
- ✓ Improves awareness and management of visitor accesses
- ✓ Simplifies the reporting process

Converged management of silos



Draft guide is online at https://nccoe.nist.gov/projects/use_cases/idam

CURRENT PROJECTS: IDAM SOLUTION



CPS Energy (San Antonio) and NCCoE are collaborating on a case study to document a worked example, lessons learned, and known benefits. Expect to complete by October.

CURRENT PROJECTS: SITUATIONAL AWARENESS

Industry Challenges:

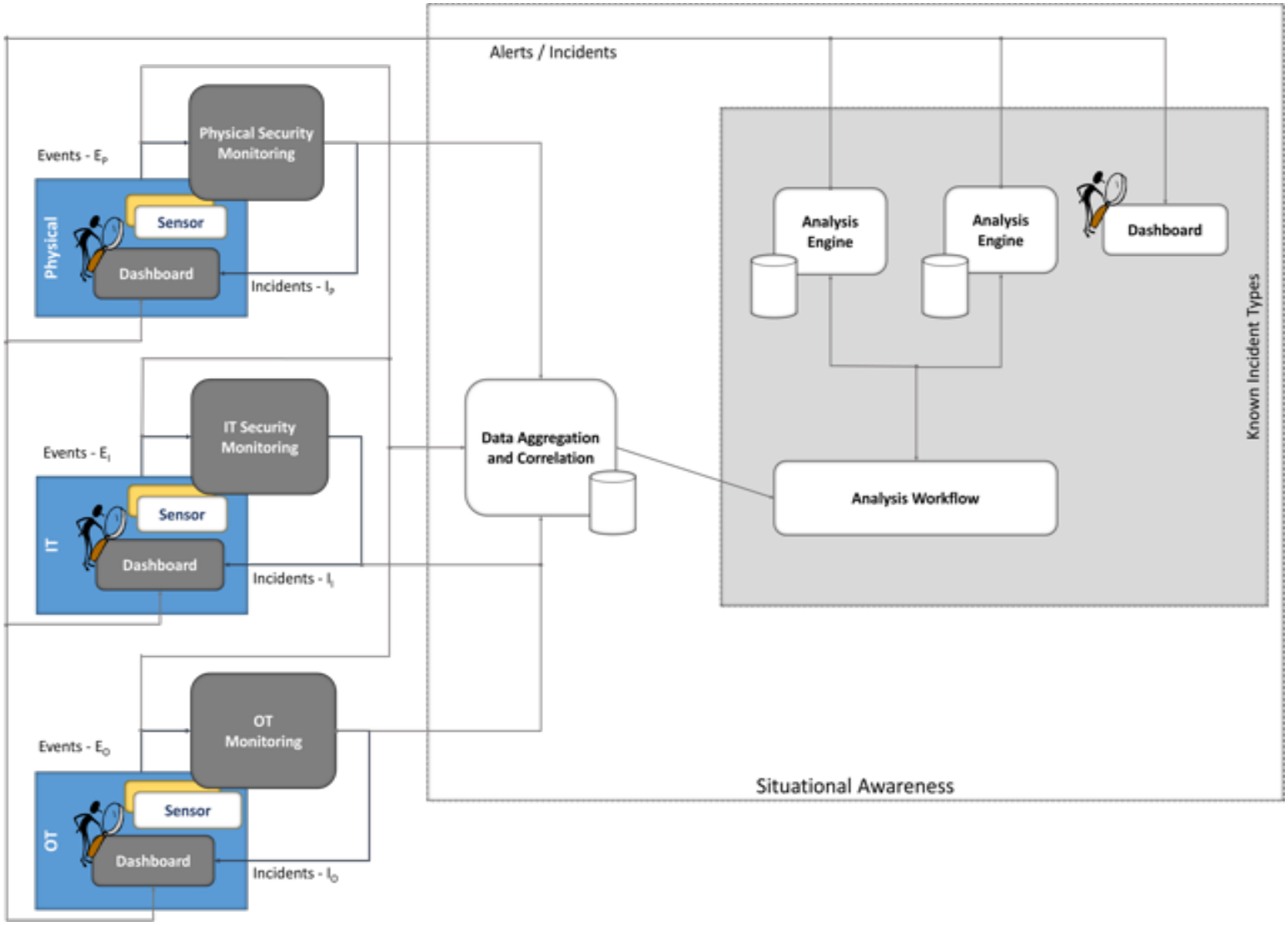
- Improve OT availability
- Detect anomalous conditions and remediation
- Unify visibility across silos
- Investigate events leading to baseline deviations/ anomalies
- Share findings

Solution NCCoE is developing:

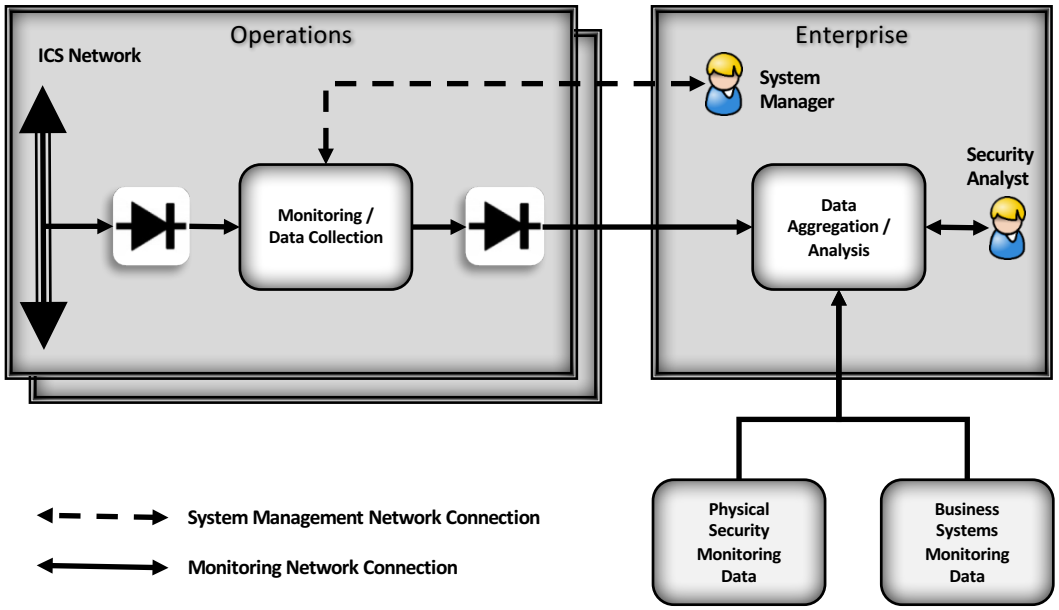
- ✓ Improves the ability to detect cyber-related security breaches or anomalous behavior
- ✓ Improves accountability and traceability
- ✓ Simplifies regulatory compliance by automating generation and collection of operational log data
- ✓ Increases the probability that investigations of attacks or anomalous system behavior will reach successful outcomes

Use Case is online at https://nccoe.nist.gov/projects/use_cases/situational_awareness

CURRENT PROJECTS: SITUATIONAL AWARENESS SOLUTION



CURRENT PROJECTS: SITUATIONAL AWARENESS



- Collect data from an Operations facility that includes Industrial Control Systems (ICS)
  - Ensure data can only flow OUT of the ICS Network into the monitoring and collection hardware / software
- Send data collected from Operations to an Enterprise data aggregation and analysis capability
  - Operations data is aggregated with business systems monitoring data and physical security monitoring data
  - Ensure data can only flow OUT of Operations into Enterprise
- Use the aggregated data to provide converged situational awareness across Operations and Business systems as well as physical security of buildings and other facilities
- Provide a limited-access remote management path from Enterprise to Operations to manage monitoring / data collection hardware and software

PROJECT MILESTONES

PROJECT NAME: IdAM	Upcoming Milestone Dates
Publish Special Publication	09/16

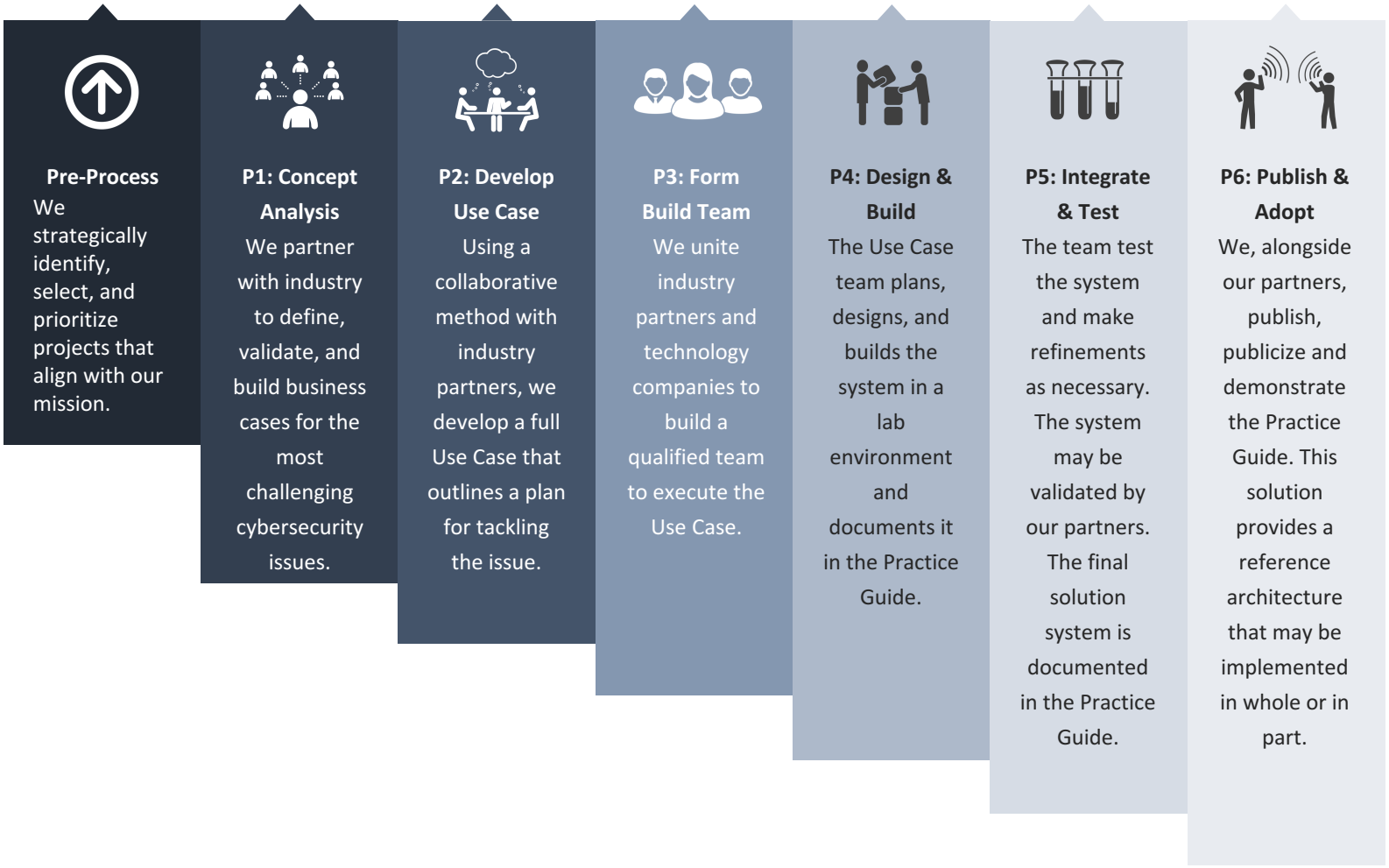
PROJECT NAME: Situational Awareness	Upcoming Milestone Dates
Completed Build	09/16
Release Draft Practice Guide for Public Comments	10/16
Publish Special Publication	03/17

PROJECT PHASES

ONG - we are here

Situational Awareness – we are here

IdAM – we are here



Pre-Process
We strategically identify, select, and prioritize projects that align with our mission.

P1: Concept Analysis
We partner with industry to define, validate, and build business cases for the most challenging cybersecurity issues.

P2: Develop Use Case
Using a collaborative method with industry partners, we develop a full Use Case that outlines a plan for tackling the issue.

P3: Form Build Team
We unite industry partners and technology companies to build a qualified team to execute the Use Case.

P4: Design & Build
The Use Case team plans, designs, and builds the system in a lab environment and documents it in the Practice Guide.

P5: Integrate & Test
The team test the system and make refinements as necessary. The system may be validated by our partners. The final solution system is documented in the Practice Guide.

P6: Publish & Adopt
We, alongside our partners, publish, publicize and demonstrate the Practice Guide. This solution provides a reference architecture that may be implemented in whole or in part.

NEW PROJECTS: ONG SUB SECTOR FOCUS

- NCCoE recognizes
  - Oil & Natural Gas (ONG) industry challenges dovetail with those of electric utilities
- NCCoE has compiled
  - emerging cybersecurity themes
    - Asset inventory and management
    - Information sharing (Situational Awareness foundational to this)
    - Supply chain risk management
    - Technology compatibility and interoperability
- NCCoE would like to develop
  - project ideas based on industry input

- The NCCoE could leverage the Situational Awareness project's inventory and access management solution and integrate a behavioral anomaly tool to demonstrate increased cybersecurity in OT systems. Additionally, the solution could pull in data from the DNG-ISAC to map a reported technology issue to a ONG system or sub-system. At an ONG site, an alert could be presented to the security operator representing a matching of a reported issue to an asset in the operator's inventory.
- Upon matching, a response may be sent to the ISAC informing them of a successful match.

- ONG faces challenges with implementing Identity and Access Management for OT and deployed enterprise systems alike.
- For example, when managing the transportation of natural gas from one location to another, authenticating access to OT or IT system access can be difficult. Vendors, suppliers and other stakeholders also need to manage revoking permissions when they are no longer needed.
- The NCCoE could research these problems and explore options providing a solution addressing IT and OT needs. Identity Federation is a key component of this activity.

- Your thoughts?

- Open Discussion

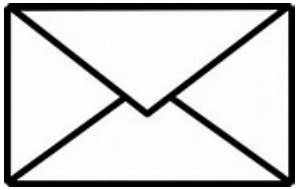
CONTACT US

301-975-0200

http://nccoe.nist.gov/forums/energy

energy_nccoe@nist.gov

9700 Great Seneca Hwy,
Rockville, MD 20850



100 Bureau Drive, Mail Stop 2002,
Gaithersburg, MD 20899

Thank You

ABOUT THE NCCOE

National Institute of Standards and Technology
U.S. Department of Commerce

Information Technology Laboratory

MARYLAND OF OPPORTUNITY.®
Department of Business & Economic Development

MONTGOMERY COUNTY
17 76
GARDEZ BIEN
MARYLAND

WHO WE ARE AND WHAT WE DO

VISION

ADVANCE CYBERSECURITY

A secure cyber infrastructure that inspires technological innovation and fosters economic growth

MISSION

ACCELERATE ADOPTION OF SECURE TECHNOLOGIES

Collaborate with innovators to provide real-world, standards-based cybersecurity capabilities that address business needs

GOAL 1

PROVIDE PRACTICAL CYBERSECURITY

Help people secure their data and digital infrastructure by equipping them with practical ways to implement standards-based cybersecurity solutions that are modular, repeatable and scalable

GOAL 2

INCREASE RATE OF ADOPTION

Enable companies to rapidly deploy commercially available cybersecurity technologies by reducing technological, educational and economic barriers to adoption

GOAL 3

ACCELERATE INNOVATION

Empower innovators to creatively address businesses' most pressing cybersecurity challenges in a state-of-the-art, collaborative environment

The NCCoE seeks problems that are:

- Broadly applicable across much of a sector, or across sectors
- Addressable through one or more reference designs built in our labs
- Complex enough that our reference designs will need to be based on a combination of multiple commercially available technologies

Reference designs address:

- Sector-specific use cases that focus on a business-driven cybersecurity problem facing a particular sector (e.g., health care, energy, financial services)
- Technology-specific building blocks that cross sector boundaries (e.g., roots of trust in mobile devices, trusted cloud computing, software asset management, attribute based access control)

TENETS

Standards-based

Apply relevant local, national and international standards to each security implementation and account for each sector's individual needs; demonstrate reference designs for new standards

Modular

Develop reference designs with individual components that can be easily substituted with alternates that offer equivalent input-output specifications

Repeatable

Enable anyone to recreate the NCCoE builds and achieve the same results by providing a complete practice guide including a reference design, bill of materials, configuration files, relevant code, diagrams, tutorials and instructions

Commercially available

Work with the technology community to identify commercially available products that can be brought together in reference designs to address challenges identified by industry

Usable

Design usable blueprints that end users can easily and cost-effectively adopt and integrate into their businesses without disrupting day-to-day operations

Open and transparent

Use open and transparent processes to complete work, and seek and incorporate public comments on NCCoE documentation, artifacts and results